# Straf- und Strafprozessrecht

## StPO § 100 a; StPO § 101 Abs. 7

**1. § 100 a StPO gestattet auch die Quellen-TKÜ mitsamt den dafür erforderlichen technischen Eingriffen in das Computersystem des Versenders.**

**2. Eine Rechtsgrundlage für das Kopieren und Speichern von grafischen Bildschirminhalten (Fertigen von Screenshots) außerhalb eines Telekommunikationsvorgangs besteht nicht. (LS des Herausgebers)**

LG Landshut, Beschluss vom 20. 1. 2011 – 4 Qs 346/10.

*Aus den Gründen:*

**I.**

**1** Mit Beschluss vom 2. 4. 2009 ordnete das Amtsgericht – Ermittlungsrichter – Landshut gemäß § 100 a StPO »die Überwachung und Aufzeichnung des Telekommunikationsverkehrs auf Ton und Schriftträger unter gleichzeitiger Schaltung einer Zählervergleichseinrichtung bzw. Herausgabe von Gesprächsverbindungsdaten und Standorte des Mobiltelefons« für den Telefonanschluss des Beschuldigten … mit der Nummer … des Netzbetreibers T-Mobile Deutschland GmbH (D) für 3 Monate bis maximal zum 2. 7. 2009 an. Ferner enthält der Beschluss folgende Aussprüche:

**2** »Mit umfasst von dieser Anordnung ist auch die Direktanwahl der Mailbox und der technischen Schaltung.

**3** Angeordnet wird insbesondere auch die Überwachung und Aufzeichnung der über den oben genannten Anschluss geführten verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen im Rahmen einer Fernsteuerung.

**4** Angeordnet wird auch die Überwachung des verschlüsselten Telekommunikationsverkehrs über HTTPS und der verschlüsselte Telekommunikationsverkehr über Messenger wie z. B. Skype.

**5** Auch insoweit sind nur solche Maßnahmen zulässig, die der Überwachung der Telekommunikation dienen und die für die technische Umsetzung der Überwachung zwingend erforderlich sind. Unzulässig sind die Durchsuchung eines Computers nach bestimmten auf diesem gespeicherten Daten sowie das Kopieren und Übertragen von Daten von einem Computer, die nicht die Telekommunikation des Beschuldigten über das Internet mittels Voice-over-IP betreffen. Auch das Abhören von Gesprächen, die außerhalb eines Telekommunikationsvorgangs im Sinne des § 100 a StPO erfolgen, ist unzulässig.«

…

**7** Der Beschluss wurde im Auftrag der Staatsanwaltschaft Landshut von den Polizeibehörden vollzogen. Hierzu hat das Bayerische Landeskriminalamt zum Zwecke der Ausleitung der verschlüsselten Telekommunikation auf dem Computer des Beschuldigten … eine Software aufgebracht, welche über zwei Überwachungsfunktionen verfügt: Die Überwachung und Ausleitung der verschlüsselten Skype-Kommunikation (Voice-over-IP sowie Chat) vor der Ver- bzw. nach der Entschlüsselung sowie das Erstellen von Screenshots der Skype-Software sowie des Internet-Browsers Firefox im Intervall von 30 Sekunden zur Überwachung der über https geführten Telekommunikation. Diese Maßnahmen wurden sodann auch umgesetzt.

**8** Der Beschuldigte wurde von den durchgeführten Telekommunikationsmaßnahmen nicht unterrichtet.

**9** Mit Schriftsatz seines Verteidigers vom 2. 3. 2010 beantragte der Beschuldigte beim Amtsgericht Landshut gemäß § 101 Abs. 7 Satz 2 StPO die Rechtswidrigkeit der Maßnahme des Beschlusses vom 2. 4. 2009 des Amtsgerichts Landshut festzustellen. …

**10** Mit Beschluss des Amtsgerichts – Ermittlungsrichter – Landshut vom 4. 10. 2010 wurde der Antrag des Beschuldigten auf gerichtliche Entscheidung als unbegründet zurückgewiesen. …

**II.**

**13** Die sofortige Beschwerde des Beschuldigten … ist gemäß §§ 101 Abs. 7 Satz 3, 311 Abs. 2 StPO zulässig und hat in der Sache teilweise Erfolg. Zwar ist der Beschluss des Amtsgerichts vom 2. 4. 2009 nicht rechtswidrig, wohl aber seine Umsetzung, soweit die grafischen Bildschirminhalte kopiert, also sog. Screenshots gefertigt wurden.

**14** 1. Der Beschuldigte war einer Katalogtat gemäß § 100 a Abs. 2 Nr. 7 a und b StPO hinreichend verdächtig… (wird ausgeführt)

**15** 2. Es ist von Rechts wegen auch nicht zu beanstanden, dass das Amtsgericht mit Beschluss vom 2. 4. 2009 neben der allgemeinen Telefonüberwachung auch die Überwachung der verschlüsselten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen im Rahmen einer »Fernsteuerung« angeordnet hat. Auf die zutreffenden Ausführungen im Beschluss des Amtsgerichts Landshut vom 2. 4. 2009, die sich die Kammer zu Eigen macht, wird Bezug genommen.

**16** Mit einer weit verbreiteten Meinung in Rechtsprechung und Literatur ist auch die Kammer der Auffassung, dass die sogenannte Quellen-TKÜ einschließlich der hierfür erforderlichen technischen Maßnahmen zulässig ist (LG Hamburg vom 31. 8. 2010, Aktenzeichen 608 Qs 17/10; KMR/Bär § 100 a StPO Rdn. 31 b f.; Meyer-Goßner 53. Aufl., § 100 a StPO Rdn. 7 ; KK-StPO/Nack, 6. Aufl., § 100 a Rdn. 27; Beck OK-StPO/Graf § 100 a StPO Rdn. 114 ff.; AG Bayreuth MMR 2010, 266). Denn § 100 a StPO erfasst grundsätzlich die Überwachung und Aufzeichnung aller vom Beschuldigten im Rahmen von Telekommunikationsvorgängen zum Zwecke dieser Kommunikation produzierten und für die Weiterleitung an den Kommunikationspartner vorgesehenen Daten. Aus rechtlicher Sicht unproblematisch ist die Überwachung und Aufzeichnung der bereits versendeten Daten. Diese ist aber praktisch wertlos, wenn die Daten vorher verschlüsselt werden. Um auch in einem solchen Fall die Überwachung der Telekommunikation gewährleisten zu können, ist es unabdingbar, bereits vor der Verschlüsselung und somit vor der Absendung auf die Audiodaten zuzugreifen. Andernfalls würde – gerade im Bereich der weit verbreiteten Internettelefonie – eine Vielzahl von Telekommunikationsvorgängen durch Maßnahmen gemäß § 100 a StPO nicht überwacht werden können. Dieser Umstand schafft denn auch eine »Annexkompetenz« für den technischen Eingriff in das Computersystem des Versenders mittels eines aufgespielten Computerprogramms (vgl. LG Hamburg a. a. O.). Für den Bereich der Internettelefonie (Voice-over-IP-Kommunikation) wird eine solche »Quellen-TKÜ« demnach von einer weit verbreiteten Meinung auch für zulässig erachtet (siehe oben).

**17** 3. Jedoch war der Vollzug des Beschlusses vom 2. 4. 2009 insoweit rechtswidrig als im zeitlichen Abstand von 30 Sekunden Screenshots von der Bildschirmoberfläche gefertigt wurden, während der Internet-Browser aktiv geschaltet war. Denn nach Auffassung der Kammer besteht für das Kopieren und Speichern der grafischen Bildschirminhalte, also der Fertigung von Screenshots, keine Rechtsgrundlage, weil zum Zeitpunkt dieser Maßnahmen noch kein Telekommunikationsvorgang stattfindet.

**18** Dabei hat die Kammer nicht verkannt, dass sich beim

verschlüsselten E-Mail-Verkehr dieselben technischen Probleme wie bei der Internettelefonie stellen, nämlich, dass nach Versenden der E-Mail eine Entschlüsselung nicht möglich ist, weshalb eine Telekommunikationsüberwachung wertlos ist. Doch kann nicht außer Acht gelassen werden, dass – anders als bei der Internettelefonie – die E-Mail zum Zeitpunkt ihrer »Ablichtung« mittels »Screenshot« noch nicht unmittelbar vor ihrer Versendung steht, insbesondere auch wieder geändert oder gelöscht werden könnte. Zwar muss der Beschuldigte um eine E-Mail verfassen zu können, eine Verbindung zu einem Server aufbauen, der ihm die erforderliche Maske zur Verfügung stellt. Der Vorgang des Schreibens der E-Mail findet dann aber ohne Datenaustausch statt, da die einzelnen Buchstaben nicht sofort an den Server weiter übertragen werden. Die E-Mail wird erst dann zum Server und damit in die Außenwelt transportiert, wenn der Beschuldigte den »Versenden-Button« betätigt. Hält man sich diese technischen Vorgänge vor Augen, kann nach Auffassung der Kammer – auch im Lichte der Entscheidung des Bundesverfassungsgerichts zur Unzulässigkeit der Online-Durchsuchung (NJW 2008, 822) – beim Schreiben einer E-Mail noch nicht von einem Vorgang der Telekommunikation gesprochen werden. Etwas Anderes kann auch nicht aus dem Umstand hergeleitet werden, dass der Beschuldigte zunächst, um die E-Mail schreiben zu können, eine Internetverbindung herstellt. Denn anders als beim Aufbau einer Telefonverbindung wird die Verbindung zum Server nach dem Aufruf der E-Mail-Maske nicht weiter genutzt. Beim Schreiben der E-Mail findet gerade kein Datenaustausch mit dem Server statt. Es kann auch nicht davon gesprochen werden, dass das Schreiben der E-Mail so eng mit ihrer späteren Versendung verknüpft ist, dass bereits das Schreiben in der Maske ohne Datenaustausch ein Vorgang der Telekommunikation im Sinne des § 100 a StPO wäre. Dies zeigt sich schon darin, dass die E-Mail während und nach dem Schreiben stets noch geändert oder gelöscht werden kann. . .

**Anmerkung**

Die *Quellen-Telekommunikationsüberwachung* (Quellen-TKÜ) hat einen heimlichen Siegeszug angetreten. Diese verdeckte Ermittlungsmaßnahme wird von der Praxis mehr und mehr bedenkenlos auf §§ 100 a, 100 b StPO gestützt.[1] Dem folgte nun auch der Ermittlungsrichter am AG Landshut und wurde insoweit – im Verfahren der sofortigen Beschwerde nach §§ 101 Abs. 7 S. 3, 311 StPO – durch das LG Landshut mit Beschluss vom 20. 1. 2011 bestätigt. Das allein böte schon genügend Anlass zur Kritik. Der dem Beschluss zugrunde liegende Sachverhalt und die forensische Analyse[2] der hier und in weiteren Fällen eingesetzten Spionagesoftware verdeutlichen darüber hinaus, dass sich die gerufenen Geister – sprich: die Quellen-TKÜ – keineswegs so leicht rechtlich und technisch bändigen lassen, wie dies von deren Befürwortern postuliert wird.

## I. Verschlüsselte Internetkommunikation – ein praktisches Problem

Die Verlagerung der Post- und Telekommunikation von analogen auf digitale, Internet-gestützte Pfade wie etwa E-Mail, Voice-over-IP (VoIP) oder Skype ist eine ungebrochene Entwicklung, die jedoch in einer ersten Stufe sogar mit einer *Erleichterung* für die Strafverfolgungsbehörden verbunden ist: Digitalisierte Kommunikationsinhalte lassen sich nämlich einfach zu Beweiszwecken sichern und später reproduzieren.[3] So können etliche digitale Telefonate und vor allem die meisten Besuche auf Webseiten[4] überwacht werden, indem die Internetkommunikation vom Telekommunikationsnetzbetreiber – z. B. dem jeweiligen DSL-Anbieter – ausgelesen und an die Strafverfolgungsbehörden übermittelt wird. Rechtlich ist das ohne weiteres auf §§ 100 a, 100 b StPO i. V. m. §§ 3 ff. TKÜV zu stützen.

Schwierigkeiten für die Strafverfolgungspraxis bereitet nun aber die zweite Entwicklungsstufe, die *Verschlüsselung* der übertragenen digitalen Daten. Gleichwohl ist dieser Trend – auch aus kriminalpräventiver Sicht – dringend geboten, denn unverschlüsselte Kommunikation ist hoch riskant, weil sie etwa die Manipulation von Finanztransaktionen (»Phishing«) erleichtert und Wirtschaftsspionage sowie andere Eingriffe in die Vertraulichkeit informationstechnischer Systeme ermöglicht. Greifen Strafverfolgungsbehörden verschlüsselte Daten wie bei einer herkömmlichen TKÜ auf dem Übertragungsweg ab, so ist jeglicher Versuch, diese Daten zu entschlüsseln, nahezu aussichtslos: Für die Kommunikationsverschlüsselung werden nämlich zumeist automatisch generierte, temporäre Schlüssel mit großer Länge und hoher Zufälligkeit verwendet.[5] Ein Ausprobieren, bis der richtige Schlüssel gefunden ist (so genannter *brute force-attack*), dauert durchschnittlich zig Jahre und ist daher hier[6] kein erfolgversprechendes Mittel. Um daher eine TKÜ – die sich in etlichen Bereichen mittlerer und schwerer Kriminalität als unverzichtbares Ermittlungsinstrument erwiesen hat – auch bei verschlüsselter Kommunikation durchführen zu können, ist nach technisch praktikablen und rechtlich tragfähigen Möglichkeiten zu suchen, diese Kommunikationsverschlüsselung zu überwinden.

## II. Lauschangriff, Man-in-the-Middle und Quellen-TKÜ: Ansätze zur Überwindung der Kommunikationsverschlüsselung

*1. Abgreifen an der Gegenstelle.* Der technisch und rechtlich[7] einfachste Weg ist es, verschlüsselte Kommunikation bei der

1 LG Hamburg wistra 2011, 155; AG Bayreuth MMR 2010, 266 m. zust. Anm. Bär sowie aus der – im Umfang unklaren – Schar unveröffentlichter Beschlüsse diejenigen des Ermittlungsrichters des BGH und des AG München (vgl. Buermeyer/Bäcker HRRS 2009, 433, 435 bei und mit Fn. 11).

2 Rieger FAS Nr. 40 vom 9. 10. 2011, S. 41; http://www.ccc.de/updates/2011/staatstrojaner (Stand: 16. 10. 2011).

3 Digitale Kopien sind nämlich in ihrem Gedankeninhalt dem Original identisch.

4 Namentlich unter Verwendung der Telefonie-Protokolle SIP und ISDN sowie des Internetprotokolls http, die allesamt keine oder keine obligatorische Verschlüsselung vorsehen.

5 Brodowski/Freiling Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 126.

6 Anders bei verschlüsselten Datenträgern, denn hier werden oft vom Benutzer vergebene und daher meist wenig zufällige Schlüssel verwendet (vertiefend Brodowski/Freiling [Fn. 5] S. 126, auch zu forensischen Alternativen; instruktiv ferner http://xkcd.com/936/[Stand: 16. 10. 2011]).

7 Aus rechtlicher Sicht besteht Streit vor allem in der Frage, ob in sämtlichen derartigen Konstellationen auf §§ 100 a, 100 b StPO zurückzugreifen ist oder ob auch eine Beschlagnahme (§§ 94 ff. StPO) ausreicht (grundlegend BVerfGE 124, 43 m. Anm. u. Bespr. Brodowski JR 2009, 402; B. Gercke StV 2009, 624; Klein NJW 2009, 2996). Zumeist nur theoretische Schwierigkeiten bereitet hingegen der Zugriff auf Daten, die im Ausland gespeichert sind: In der Regel verhalten sich nämlich große, international tätige E-Mail-Provider ausgesprochen kooperativ und geben deutschen Strafverfolgungsbehörden auch diese Daten heraus. Alternativ wäre aufgrund der völkerrechtlichen Implikationen ein Rechtshilfeersuchen zu stellen; vgl. zum insoweit vergleich-

Gegenstelle abzugreifen, denn dort wird sie ohnehin wieder entschlüsselt. Verwendet etwa ein Verdächtiger eine verschlüsselte Internetverbindung, um in seinem Postfach lagernde E-Mails zu lesen, so ist der einfachste und schnellste Weg, auf die bei seinem E-Mail-Provider in unverschlüsselter Form vorliegenden Nachrichten zuzugreifen. Dieser Ansatz scheitert lediglich dann, wenn die Gegenstelle nicht kooperativ ist oder wenn Anlass zur Sorge besteht, diese könnte mit dem Beschuldigten zusammenwirken. Das ist etwa dann der Fall, wenn der Beschuldigte die Software Skype für Internettelefonie oder für Chatnachrichten verwendet, denn diese verschlüsselt die Nachrichten grundsätzlich[8] vom einen bis zum anderen Kommunikationspartner (*end-to-end*).

*2. Man-in-the-Middle.* Ein Man-in-the-Middle-System ist ein informationstechnisches System, das zwischen die beiden Gegenstellen geschaltet wird und ihnen das jeweilige Gegenüber vortäuscht.[9] Um ein solches System einzusetzen, muss erstens das vom Verdächtigen genutzte Computersystem mit falschen, über das Netzwerk gesendeten Daten dazu gebracht werden, das Man-in-the-Middle-System anstelle[10] der korrekten Gegenstelle zu kontaktieren.[11] Zweitens muss dessen Rechner über die Identität der Kommunikationsgegenstelle getäuscht werden. Das hierfür benötigte, falsche Authentifizierungszertifikat muss dazu von einer als vertrauenswürdig eingestuften[12] Agentur signiert werden.[13] Diesen Weg beschritten im Sommer 2011 mutmaßlich iranische Sicherheitsbehörden, um auf E-Mail-Postfächer zuzugreifen, die vermeintlich sicher vor deren Zugriffen u. a. bei Google angelegt waren.[14]

Die überragende Bedeutung verlässlicher Authentifizierungsmechanismen für das Internet – etwa für sicheres Online-Banking – führt aber zur technischen Abhärtung gegen *man-in-the-middle*-Angriffe und folglich dazu, dass diese in Zukunft technisch noch schwieriger realisierbar sein dürften als bisher. Aus rechtlicher Sicht ist zudem auf die erheblichen Kollateralschäden dieser Herangehensweise – so für das generelle Vertrauen in die korrekte Arbeit der Authentifizierungsagenturen – und auf die Gefahr hinzuweisen, dass die Überwachung vorschnell entdeckt werden könnte, weil neuartige Sicherheitstechnologien dem Betroffenen Alarm schlagen.[15]

*3. »Obligatorische Entschlüsselungstechnologien«.* Gelegentlich werden Forderungen laut, dass sämtliche Verschlüsselungssoftware und -hardware einen Zweitschlüssel für staatliche Zugriffe vorsehen müsse.[16] Abgesehen davon, dass sich diese Forderung ohnehin praktisch nicht umsetzen ließe,[17] böte eine solche Hintertür zum einen das erhebliche Risiko, dass sie von Kriminellen entdeckt und ausgenutzt werden könnte. Zum anderen führte allein deren Existenz zu einem generellen Gefühl des Überwacht-Seins, das sich nicht nur auf die äußeren Umstände der Kommunikation,[18] sondern auch auf deren Inhalte bezöge, welche aus staatlicher Seite »mit nur einem Mausklick« abgegriffen werden könnten. »Obligatorische Entschlüsselungstechnologien« bergen daher die Gefahr zu übermäßig konformen, angepasstem Verhalten und daher zur reduzierten Teilhabe am freiheitlich-demokratischen Gemeinwesen.[19] Aus verfassungsrechtlicher Sicht sind daher »obligatorische Entschlüsselungstechnologien« nicht einmal ansatzweise diskutabel.

Entschließt sich jedoch ein Softwareanbieter aus freien Stücken, eine solche Hintertür in seiner Software bereitzuhalten,[20] so kann deren Verwendung auf §§ 100 a, 100 b StPO gestützt werden. Dies greift dann nicht zusätzlich[21] in die Vertraulichkeit und Integrität des vom Betroffenen verwendeten informationstechnischen Systems ein. Etliche Indizien weisen darauf hin, dass auf diesem Weg zumindest manche Ermittlungsbehörden mancher Staaten Zugriff auf Skype-Telefonate erlangen können.[22]

*4. »Großer« und »kleiner« Lauschangriff (§§ 100 c–100 f StPO).* Im Rahmen einer Wohnraumüberwachung (§§ 100 c–100 e StPO) kann auch das, was ein Verdächtiger in ein (Computer-) Telefon spricht – und auch das, was er hört[23] – mittels im Raum installierter »Wanzen« abgehört und aufgezeichnet werden. Entsprechend kann auch das, was er außerhalb der besonders geschützten Räumlichkeiten – etwa in ein Skype-fähiges Mobiltelefon – spricht, mittels des »kleinen Lauschangriffs« (§ 100 f StPO) abgehört werden.

*Außerhalb* des räumlich durch Art. 13 GG, §§ 100 c–100 e StPO besonders geschützten Bereichs steht daher den Ermittlungsbehörden mit § 100 f StPO ein probates technisches Mittel zur Verfügung, um verschlüsselte Telefonate »an der Quelle«

baren § 110 Abs. 3 StPO nur Bär ZIS 2011, 55; Schmitt in: Meyer-Goßner StPO, 54. Aufl. 2011, § 110 Rdn. 7 a.

**8** Siehe aber noch unten II.3. bei und mit Fn. 22.

**9** So suggeriert dieses System beispielsweise dem Verdächtigen, dass dies die Webseite des E-Mail-Providers sei; diesem wiederum suggeriert das System, dass es selbst der legitime Kunde sei. Auf diese Weise erhält das Man-in-the-Middle-System Kenntnis der unverschlüsselten Kommunikation zwischen den Gegenstellen.

**10** Kriminelle umgehen dies bisweilen auch dadurch, dass Opfer auf ähnlich lautende Internetadressen gelockt werden.

**11** Hierzu ließe sich der Netzbetreiber auch verpflichten, § 100 b Abs. 3 S. 1 StPO.

**12** Diese Einstufung erfolgt durch die Betriebssystem- und Browser-Softwareentwickler. Dabei handelt es sich inzwischen um eine Liste mit Hunderten von Anbietern, die teilweise auch aus dem exekutiven Umfeld – auch nicht über alle Zweifel erhabener – Staaten stammen.

**13** Ob eine solche Mitwirkung einer Agentur gem. § 100 b Abs. 3 S. 1 StPO verlangt werden könnte, ist zweifelhaft: Bei Bekanntwerden eines solchen falschen Zertifikats – und damit ist auch bei verdeckten Überwachungsmaßnahmen zu rechnen – droht der Agentur nämlich der wirtschaftliche Ruin, was die Anordnung der Mitwirkung unverhältnismäßig werden lässt.

**14** Die niederländische Zertifikateagentur DigiNotar gab Anfang September 2011 bekannt, dass es ab Juli 2011 Angreifern gelungen war, eine Signatur von DigiNotar unter falsche Zertifikate u. a. von google.com zu erlangen. Ein Auswertungsbericht von Fox-IT berichtet detailliert davon, dass die Spurenlage auf einen Angriff aus dem Iran hinweist, http://bit.ly/plPF7P (Stand: 16. 10. 2011).

**15** Dies führte auch zur Entdeckung des soeben Fn. 14 geschilderten Vorfalls.

**16** Zuletzt etwa die Kommission zur Evaluierung der Sicherheitsbehörden in ihrem Abschlussbericht; Werthebach u. a., Kooperative Sicherheit – Die Sonderpolizeien des Bundes im föderalen Staat, 2010, S. 131.

**17** Effektive Verschlüsselungstechnologie lässt sich schließlich auch aus ausländischen Quellen und über das Internet beziehen.

**18** Wie bei der höchst umstrittenen, anlasslosen Vorratsdatenspeicherung von Verbindungsdaten, vgl. BVerfGE 125, 260.

**19** Vgl. BVerfGE 65, 1, 43.

**20** Ob er sich in diesem Fall gegenüber seinen Kunden pflichtwidrig verhält, ist eine primär zivilrechtlich zu beurteilende Frage.

**21** Die Vertraulichkeit und Integrität des informationstechnischen Systems ist bereits seit der Installation der derart mit einem Makel behafteten Software betroffen. Soweit dies jedoch nicht auf – auch mittelbarer – staatlicher Veranlassung beruht, ist kein staatlicher Eingriff in den Schutzbereich dieses Grundrechts zu sehen.

**22** Becker/Meinicke StV 2011, 50, 51; Buermeyer/Bäcker HRRS 2009, 433, 434 m. Nachw.; Braun K&R 2011, 681, 685.

**23** Erstens könnten diese Aussagen am jeweils überwachten Ort von einem dort hypothetisch anwesenden Ermittlungsbeamten wahrgenommen werden. Zweitens sind §§ 100 a, 100 b StPO einerseits und §§ 100 c–100 f StPO andererseits nur unterschiedliche Ausprägungen des Schutzes von Kommunikation. Zwar basiert die Schutzbedürftigkeit auf anderen Grundrechten, doch im Lichte des gemeinsamen Kerns überrascht es nicht, dass § 100 f StPO dieselben Schutzstandards setzt wie §§ 100 a, 100 b StPO und §§ 100 c–100 e StPO hierüber noch hinausgeht.

abzuhören. Da die Hürden zur Anordnung denen einer TKÜ nach §§ 100 a, 100 b StPO nahezu[24] entsprechen, ist eine Quellen-TKÜ durch technische Manipulation des Endgeräts daher weder aus technischer noch aus rechtlicher Sicht erforderlich. Telefoniert ein Beschuldigter aber *in einer Wohnung*, so erscheint es auf den ersten Blick als widersprüchlich, dass ein herkömmliches Telefonat nach §§ 100 a, 100 b StPO abgehört werden kann, ein verschlüsseltes jedoch nur unter den höheren Hürden der §§ 100 c–100 e StPO (u. a. engerer Straftatenkatalog, zwingender Richtervorbehalt).

*5. Quellen-TKÜ.* Unter einer Quellen-TKÜ versteht man das Abgreifen der digitalen, aber noch nicht verschlüsselten Kommunikationsinhalte bereits am Rechner eines Verdächtigen oder Nachrichtenmittlers, die sodann an die Strafverfolgungsbehörden übermittelt werden. Kann dies nicht über eine vom Softwareanbieter eingebaute Hintertür erfolgen,[25] müssen die Strafverfolgungsbehörden für eine solche Manipulation die *vollständige*[26] Herrschaft über das informationstechnische System des Betroffenen erlangen (Administratorenrechte) und eine Spionagesoftware (*Remote Forensic Software*) installieren. Um dies zu bewerkstelligen, ist ein (kurzzeitiger) physischer Zugriff auf das informationstechnische System äußerst hilfreich.[27] Das kann – wenn auch rechtlich unzulässig – bei einem heimlichen Betreten der Wohnung des Betroffenen geschehen, oder etwa, wie hier, während einer Zollkontrolle am Flughafen.[28]

## III. Quellen-TKÜ und §§ 100 a, 100 b StPO: Ein missverstandes *obiter dictum* und eine zweifelhafte »h. M.«

Bietet nun eine Quellen-TKÜ den von den Ermittlungsbehörden erhofften Ausweg aus dem Verschlüsselungs-Dilemma? Das LG Landshut – wie auch zuvor schon der Ermittlungsrichter am AG Landshut – ist dieser Auffassung und verweist knapp auf eine »weit verbreitete[…] Meinung in Rechtsprechung und Literatur …, dass die sogenannte Quellen-TKÜ einschließlich der hierfür erforderlichen technischen Maßnahmen« nach §§ 100 a, 100 b StPO zulässig sei. Das hierbei von der Rechtsprechung[29] und den judikativ geprägten[30] Teilen der Literatur herangezogene *obiter dictum* des BVerfG trägt dieses Ergebnis jedoch nicht: §§ 100 a, 100 b StPO ist keine verfassungsrechtlich tragfähige, normenklare und -bestimmte[31] Eingriffsnorm für einen derart missbrauchsanfälligen und grundrechtssensiblen Eingriff.

1. Das Urteil des BVerfG zur Verfassungswidrigkeit der Bestimmungen des nordrhein-westfälischen Verfassungsschutzgesetzes über die präventive Online-Durchsuchung[32] enthält kein klares Votum zu einer auf §§ 100 a, 100 b StPO gestützten, repressiven Quellen-TKÜ.

Das BVerfG weist zunächst prominent auf die erheblichen Gefahren hin, die mit einer Infiltration und der Installation eines Spionageprogramms auf einem informationstechnischen System verbunden sind: Hiermit sei »die entscheidende Hürde genommen, um das System insgesamt auszuspähen.… Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Erfasst werden können beispielsweise das Verhalten bei der Bedienung eines Personalcomputers für eigene Zwecke, die Abrufhäufigkeit bestimmter Dienste, insbesondere auch der Inhalt angelegter Dateien oder – soweit das infiltrierte informationstechnische System auch Geräte im Haushalt steuert – das Verhalten in der eigenen Wohnung.«[33] Man muss ergänzen: Auch kann dies zur verdeckten akustischen und optischen (Wohnraum-)Überwachung missbraucht werden.[34]

Gestützt auf diese Gefahrenlage definiert das BVerfG sodann den grundrechtlichen Prüfungsmaßstab: Bei einer Quellen-TKÜ bestehe »stets … das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit … kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden.« Daher könne nur dann »Art. 10 Abs. 1 GG … der alleinige Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-TKÜ [sein], wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein.«[35]

2. Genügen §§ 100 a, 100 b StPO diesen verfassungsrechtlichen Anforderungen?

a) Beträchtliche Stimmen in der Literatur verweisen seit längerem darauf, dass eine Quellen-TKÜ unter Einsatz einer Spionagesoftware technisch gerade nicht die Gewähr dafür bietet, dass »ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang« zugegriffen wird.[36] Die hierfür notwendige Übernahme von Administratorenrechten ist nämlich unbe-

**24** Einziger materieller Unterschied ist, dass § 100 f StPO nicht anwendbar ist, wenn ein Beschuldigter eine Katalogtat »durch eine Straftat« vorbereitet hat (so aber § 100 a Abs. 1 Nr. 1 a. E.).

**25** Zu den damit verbundenen, erheblichen rechtlichen Implikationen siehe bereits oben II.3. bei und mit Fn. 21.

**26** Nur so lassen sich nämlich vorhandene Schutzmechanismen – etwa ein »Virenscanner« – umgehen.

**27** Alternativ kann auch über eine Internetverbindung versucht werden, den Rechner des Beschuldigten zu kapern – was allerdings mit dem Risiko erheblicher Kollateralschäden verbunden ist – oder dieser durch »social engineering« dazu gebracht werden, die Spionagesoftware zu installieren. Zu diesen und anderen Infiltrationsmöglichkeiten vgl. bereits Buermeyer HRRS 2007, 154.

**28** BT-Prot. 17/132, S. 15597 (A).

**29** S. oben bei und mit Fn. 1.

**30** Bei aller Frage, welches diskursive Gewicht Verweise der Rechtsprechung auf die Literatur haben bzw. haben sollen und wie eine »h. M.« festzustellen ist, sei an dieser Stelle angemerkt: Das LG Landshut verweist hier nur auf solche Stimmen in der Literatur, die zugleich hohe Richterämter innehaben: Bär in: KMR-StPO, § 100 a Rdn. 31 b f.; Meyer-Goßner/Schmitt (Fn. 7) § 100 a Rdn. 7 a; Nack in: Karlsruher Kommentar zur StPO, 6. Aufl. 2008, § 100 a Rdn. 27 sowie Graf in: Beck'scher Online-Kommentar StPO, 2011, § 100 a Rdn. 114 ff. Keine Erwähnung finden jedoch die kritischen Stimmen von Strafverteidigern und Rechtswissenschaftlern, die sich mit demselben Rechtsproblem beschäftigt haben, namentlich Becker/Meinicke StV 2011, 50; Th. Böckenförde JZ 2008, 925, 934 bei und mit Fn. 96; Buermeyer/Bäcker HRRS 2009, 433, 440; Hoffmann-Riem JZ 2008, 1009, 1022; Hornung CR 2008, 299, 300 f.; Vogel/Brodowski StV 2009, 632, 634; Wolter in: SK StPO, 4. Aufl. 2010, § 100 a Rdn. 27 ff. Ferner sei auf die erst nach dem Beschluss veröffentlichten, kritischen Beiträge von Abate DuD 2011, 122, 125; F. Albrecht JurPC Web-Dok. 59/2011 Abs. 12 ff.; Braun jurisPR-ITR 3/2011 Anm. 3; ders. K&R 2011, 681 verwiesen.

**31** Vgl. BVerfGE 110, 33, 52 ff.; BVerfGE 120, 274, 315 ff.

**32** BVerfGE 120, 274 m. Anm. u. Bespr. Bär MMR 2008, 327; Th. Böckenförde JZ 2008, 925; Britz DÖV 2008, 411; Hornick StraFo 2008, 281; Hornung CR 2008, 299; Kutscha NJW 2008, 1042; Michalke StraFo 2008, 287; Petri DuD 2008, 443; Rossnagel/Schnabel NJW 2008, 3534; Sachs/Krings JuS 2008, 481.

**33** BVerfGE 120, 274, 308 f.

**34** Zutr. Becker/Meinicke StV 2011, 50, 51 bei und mit Fn. 18.

**35** BVerfGE 120, 274, 309.

**36** Becker/Meinicke StV 2011, 50, 51; Buermeyer/Bäcker HRRS 2009, 433, 439; Hoffmann-Riem JZ 2008, 1009, 1022; Hornung CR 2008, 299, 300 f.; Vogel/Brodowski StV 2009, 632, 634.

schränkt, so dass Tür und Tor für exzessive Datenzugriffe offen stehen. Die von der Rechtsprechung vertretene Gegenauffassung verweist hingegen darauf, dass durch »zweckentsprechende Programmierung« sichergestellt werden könne, dass exzessive Datenzugriffe unterbleiben.[37] Das jedoch ist keine *technische,* sondern nur eine organisatorische Vorkehrung.[38] Dass dieses technische Risiko nicht nur eine theoretische Gefahr darstellt, sondern sich auch in der Praxis realisiert, verdeutlicht diese Entscheidung des LG Landshut:

Der amtsgerichtliche Beschluss gestattet ausdrücklich die Installation einer Spionagesoftware auf dem Rechner des Beschuldigten, um dessen Skype-Telefonate abhören zu können. Hierüber hinausgehend übermittelte die Spionagesoftware alle 30 Sekunden auch einen Screenshot[39] der Skype-Software sowie des Internet-Browsers. Aus ermittlungstaktischer Sicht mag dies sinnvoll gewesen sein, um vom Beschuldigten verschlüsselt versandte Chatnachrichten oder E-Mails im unverschlüsselten Zustand ausspähen zu können. Bei den so gewonnenen Daten handelte es sich jedoch keineswegs um solche aus einem laufenden Telekommunikationsvorgang.

Das LG Landshut stellt maßgeblich und zutreffend darauf ab, dass durch solche Screenshots Daten abgegriffen werden können, die *noch nicht* Gegenstand einer Telekommunikation sind. Nach ganz herrschender Auffassung beginnt die Telekommunikation nämlich erst dann, wenn ein Kommunikationsvorgang den Herrschaftsbereich des Absenders verlassen hat.[40] Wird aber über einen Webmail-Dienst eine E-Mail oder über Skype eine Chat-Nachricht eingetippt, so wird zwar dieser noch unverschlüsselte Nachrichtentext im entsprechenden Fenster angezeigt. Die hierfür notwendigen Rechenoperationen finden jedoch ausschließlich auf dem lokalen Rechner statt. Eine Verschlüsselung und Übertragung der Nachricht an den Empfänger findet erst statt, wenn der Benutzer das Absenden der Nachricht veranlasst. Somit liegt auch erst dann eine Telekommunikation vor.[41] Neben dieser technischen ist auch die funktionale Seite zu beachten: Abgegriffen wurden schließlich nur *Entwürfe*, die vom Betroffenen ohne weiteres noch verändert oder gelöscht werden können, bevor sie erst später Gegenstand einer Kommunikation werden.[42]

Dem LG Landshut ist daher insoweit voll und ganz zuzustimmen, als dass das Abgreifen der Screenshots schon keine Quellen-TKÜ darstellte und daher rechtswidrig war. Ergänzend ist darauf hinzuweisen, dass im Anzeigefenster der Skype-Software und des Internet-Browsers auch solche Informationen angezeigt werden, die ausschließlich auf lokal abgespeicherten Daten beruhen und damit keinerlei Bezug zu einer vergangenen oder laufenden Telekommunikation aufweisen.[43] Zudem lassen sich in einem Browser auch Daten – etwa aus einem Zwischenspeicher (*Cache*) – anzeigen, die schon vor längerer Zeit übertragen wurden. Dann ist aber – zumindest nach der vorherrschenden Auffassung – der diese Daten betreffende Telekommunikationsvorgang bereits beendet.[44]

Darüber hinausgehend konnte der Chaos Computer Club in seiner forensischen Analyse überzeugend belegen, dass die von mehreren Bundesländern und auch in diesem Fall zur Quellen-TKÜ verwendete Software alles andere als »zweckentsprechend« programmiert ist: Über die – rechtswidrige – Funktionalität des Anfertigens der Screenshots hinaus konnten die Strafverfolgungsbehörden nach Belieben weitere Überwachungsmodule nachträglich installieren und hätten so etwa auch eine akustische oder optische Wohnraumüberwachung vornehmen können.[45] Die eingesetzte Software bietet daher gerade nicht die vom BVerfG geforderte Gewähr dafür, dass exzessive Datenzugriffe *technisch* ausgeschlossen sind. Aus demselben Grund dürfte auch eine korrekt programmierte Spionagesoftware keine Aktualisierungsfunktion vorsehen.

b) Kann die Beschränkung der Datenerhebung auf laufende Telekommunikationsvorgänge durch § 100 b Abs. 2 S. 2 Nr. 3 StPO, demzufolge »Art, Umfang und Dauer« einer TKÜ schriftlich zu fixieren seien, rechtlich gewährleistet werden? Hiervon geht die Rechtsprechung[46] und auch (implizit) das LG Landshut aus. Leitbild des § 100 b Abs. 2 S. 2 Nr. 3 StPO ist es jedoch, die konkrete Ausgestaltung einer TKÜ weiter zu begrenzen, um deren Verhältnismäßigkeit zu wahren.[47] Normalfälle hierfür wären die Begrenzung einer TKÜ auf bestimmte angewählte Telefonnummern oder auf Telefonate, die zur Nachtzeit geführt werden. Eine verfassungskonforme Quellen-TKÜ betrifft hingegen weniger die konkrete Ausgestaltung der TKÜ selbst, sondern vorrangig das vorgeschaltete Problem, wie die technische Maßnahme *auf* eine TKÜ begrenzt werden kann. Diese Fragen thematisiert § 100 b Abs. 2 S. 2 Nr. 3 StPO in keiner Weise. Daher ist im Lichte der Wesentlichkeitstheorie eine Entscheidung des Gesetzgebers zu verlangen.[48]

c) Aufgrund der fehlenden technischen Vorkehrungen und rechtlichen Vorgaben, um den Datenabgriff auf laufende Telekommunikation zu beschränken, ist die Infiltration des Rechners durch die Installation einer Spionagesoftware und damit der für eine Quellen-TKÜ notwendige Begleiteingriff nicht nur

**37** LG Hamburg wistra 2011, 155, 158.

**38** Braun jurisPR-ITR 3/2011 Anm. 3 sieht hierin jedoch einen »Grundrechtsschutz durch technische Verfahren«.

**39** Dies ist eine digitale Kopie dessen, was im entsprechenden Fenster am Bildschirm angezeigt wurde.

**40** S. nur Durner in: Maunz/Dürig, GG, 62. Lfg. 2011, Art. 10 Rdn. 62 m. w. N.; anders nur Hornick StraFo 2008, 281, 284, der bereits das »Eintippen« eines E-Mail-Entwurfs als Anwendungsfall für eine Quellen-TKÜ ansieht.

**41** Aus forensischer Sicht böte es sich an, die Verschlüsselungsroutine – etwa des Internet-Browsers – dahingehend zu modifizieren, dass vorab eine Kopie der Nachrichteninhalte an die Strafverfolgungsbehörden ausgeleitet wird. Es besteht daher die technische Möglichkeit einer wirksamen Begrenzung auf laufende Telekommunikation, so dass auf das Anfertigen von Screenshots auch aus ermittlungstaktischer Sicht verzichtet werden kann.

**42** Rieger FAS Nr. 40 vom 9. 10. 2011, S. 41, 42 wirft die Frage auf, ob bei der Verwendung einer internetbasierten Textverarbeitung die dabei vom lokalen Rechner (Client) an den Server bzw. die »Cloud« gesendete Daten Telekommunikation darstellen, die gem. §§ 100 a, 100 b StPO abgegriffen werden dürfe. Hierzu ist zunächst festzuhalten, dass auch bei der bloßen Interaktion zwischen Mensch und (entfernter) Maschine Telekommunikation vorliegt und daher die §§ 100 a, 100 b StPO anwendbar sind. Dient ein Server oder die »Cloud« aber nicht als technisches Mittel zur Kommunikation mit anderen Menschen, sondern bloß als technischer Ersatz für einen lokalen Arbeitsplatzrechner, so spricht aus technisch-funktionaler Sicht (vgl. Brodowski JR 2009, 402, 403) viel dafür, einen Zugriff auf diese Client-Server-Telekommunikationsdaten nur ausgesprochen restriktiv zu gestatten.

**43** Exemplarisch sei auf lokal abgespeicherte Hilfeseiten verwiesen, zu deren Darstellung der Internet-Browser Verwendung findet.

**44** BVerfGE 106, 28, 37 f.; BVerfGE 115, 166, 183 ff.; BVerfGE 120, 274, 307 f.

**45** Rieger FAS Nr. 40 vom 9. 10. 2011, S. 41, 41 f.

**46** AG Bayreuth MMR 2010, 266; s. auch Meyer-Goßner/Schmitt (Fn. 7) § 100 a Rdn. 7 a.

**47** Der Gesetzgeber intendiert mit dieser Norm auch allein die Konkretisierung der TKÜ, vgl. BT-Drs. 15/5846, S. 47.

**48** So i. E. auch Becker/Meinicke StV 2011, 50, 51 f.; Braun jurisPR-ITR 3/2011 Anm. 3; Buermeyer/Bäcker HRRS 2009, 433; Hoffmann-Riem JZ 2008, 1009, 1022; Kudlich GA 2011, 193, 206; SK-StPO/Wolter (Fn. 30) § 100 a Rdn. 30.

an Art. 10 Abs. 1 GG zu messen,[49] sondern jedenfalls auch am Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG).[50] Für Eingriffe in dieses mitbetroffene Grundrecht bietet §§ 100 a, 100 b StPO keine Grundlage, auch nicht in Gestalt einer »Annexkompetenz«:[51] Eine Quellen-TKÜ ist aufgrund ihrer heimlich herbeigeführten, erheblichen Begleiterscheinungen gerade nicht mit einer herkömmlichen TKÜ zu vergleichen, sondern stellt eine höchst atypische Sonderform dar.

d) Diese Sichtweise lässt sich auch systematisch und historisch bestätigen: Makroystematisch sieht § 20 l Abs. 2 BKAG eine explizite Regelung für eine Quellen-TKÜ vor.[52] Diese Norm war für erforderlich gehalten worden, obwohl § 20 l Abs. 1, Abs. 3 bis 6 BKAG eine eng an §§ 100 a, 100 b StPO orientierte Regelung enthalten. Mikrosystematisch ist § 100 a StPO nicht die einzige – und daher auch keine gleichermaßen abschließende wie vollständige – Norm für Eingriffe in Art. 10 Abs. 1 GG.[53] Historisch ist darauf zu verweisen, dass bei der Neuregelung der §§ 100 a, 100 b StPO im Jahre 2007 die verfassungsrechtliche und politische Diskussion über die Zulässigkeit einer Online-Durchsuchung – und damit auch einer Quellen-TKÜ – bereits in regem Gange war, woran sich auch Bundesminister und Mitglieder des Bundestages beteiligten.[54] Das Schweigen der §§ 100 a, 100 b StPO über Fragen der Quellen-TKÜ kann daher gerade nicht als planwidrige Regelungslücke aufgefasst werden,[55] so dass es auf die – zweifelhafte – Analogiefähigkeit strafprozessualer Eingriffsbefugnisse erst gar nicht ankommt.

3. §§ 100 a, 100 b StPO taugen daher nicht als Eingriffsgrundlage für eine Quellen-TKÜ. Erforderlich ist vielmehr eine explizite, normenklare Regelung der Quellen-TKÜ durch den demokratisch legitimierten Gesetzgeber,[56] die auch die auf der Manipulation des Rechners beruhende, geringere Beweisqualität berücksichtigen müsste[57] – ganz abgesehen von der bemerkenswerten Funktionalität der im konkreten Fall eingesetzten Software, die es den Strafverfolgungsbehörden und auch Dritten ermöglicht hätte, mit wenigen Mausklicks beliebige (belastende) Dateien auf dem Rechner des Beschuldigten zu hinterlegen.[58]

Wenn als Begleiteingriff das physische Eindringen in die Wohnung des Betroffenen gestattet werden soll, um an dessen Rechner zu gelangen und diesen zu infiltrieren, ist eine solche Regelung zwingend am Schutzniveau des Art. 13 GG, §§ 100 c–100 e StPO auszurichten.[59] Viel spricht jedoch dafür, dass sich die Regelung einer Quellen-TKÜ auch generell an diesem hohen Schutzstandard orientieren müsste: Diese Maßnahme ist schließlich nur dann erforderlich, wenn ein verschlüsseltes Telefonat *in einer Wohnung* geführt wird.[60] Auch aus diesem Aspekt, der auf einer »durch die Abgrenzung der Wohnung vermittelte[n] räumliche[n] Privatsphäre« beruht, ergibt sich eine besondere, raumbezogene Schutzbedürftigkeit, wie sie nur Art. 13 GG gewährleistet.[61]

4. Trotz alledem verbleibt ein erheblicher Anwendungsbereich für die im *obiter dictum* des BVerfG thematisierte Quellen-TKÜ: Hält ein Softwareanbieter von sich aus eine Hintertür bereit, die eine Ausleitung des unverschlüsselten Datenstroms ermöglicht, so ist die Nutzung dieser Hintertür durch die Strafverfolgungsbehörden ausschließlich an §§ 100 a, 100 b StPO zu messen.[62]

## IV. Die internationale Dimension einer Quellen-TKÜ

Wird, wie hier, ein portables informationstechnisches System – etwa ein Notebook, ein Tablet oder ein Skype-fähiges Smartphone – infiltriert, so ist es oft nur eine Frage der Zeit, bis der Betroffene mit diesem Gerät ins Ausland reist. Die Fortsetzung einer Quellen-TKÜ berührt dann aber aufgrund der Eingriffsintensität der Maßnahme das völkerrechtlich geschützte Souveränitätsinteresse des ausländischen Staates. Eine Quellen-TKÜ ist daher für die Dauer des Auslandaufenthalts zu unterbrechen, es sei denn, der ausländische Staat erklärt sich im förmlichen Rechtshilfeverfahren mit der Fortsetzung der Ermittlungsmaßnahme einverstanden. Nur im Anwendungsbereich des Rechtshilfeübereinkommens von 2000 genügt gemäß dessen Art. 20 vorläufig die bloße Notifikation des ausländischen Staates, der aber die Fortsetzung der Maßnahme verbieten darf.[63] Solange jedoch keine tragfähige strafprozessuale Eingriffsgrundlage für eine Quellen-TKÜ besteht, ist es deutschen Ermittlungsbehörden ohnehin verwehrt, ausländische Stellen um die Durchführung einer solchen Maßnahme zu ersuchen (arg. ex § 77 Abs. 1);[64] eingehende Ersuchen sind bis auf weiteres abzulehnen oder durch in Deutschland zulässige, alternative Ermittlungsmaßnahmen zu erfüllen (§§ 59 Abs. 3, 77 Abs. 1 IRG).[65]

**49** BVerfGE 120, 274, 308 f.

**50** BVerfGE 120, 274, 308; bezogen auf den konkreten Fall vgl. auch Braun jurisPR-ITR 3/2011 Anm. 3.

**51** So aber LG Hamburg wistra 2011, 155, 156 ff. Grundsätzlich zu Annexkompetenzen zu strafprozessualen Eingriffsbefugnissen BGHSt 46, 266, 273 f. m. abl. Anm. Kühne JZ 2001, 1148; Schäfer in: Löwe-Rosenberg, StPO, 25. Aufl. 2004, § 100 c Rdn. 8 m. w. N.; vgl. ferner SK-StPO/Wolter (Fn. 30) § 100 a Rdn. 29.

**52** Zu diesem systematischen Argument s. auch Braun jurisPR-ITR 3/2011 Anm. 3; ders. K&R 2011, 681, 685; Buermeyer/Bäcker HRRS 2009, 433, 438; Vogel/Brodowski StV 2009, 632, 634.

**53** BVerfGE 124, 43, 58 f.; F. Albrecht JurPC Web-Dok. 59/2011 Abs. 16; Becker/Meinicke StV 2011, 50, 51; Brodowski JR 2009, 402, 407; Kudlich GA 2011, 193, 196.

**54** Exemplarisch sei auf die Äußerungen des MdB Dr. Dieter Wiefelspütz und des damaligen Bundesministers des Inneren, Dr. Wolfgang Schäuble, verwiesen, von denen am 6. 2. 2007 berichtet wurde: http://bit.ly/ox06ts (Stand: 16. 10. 2011).

**55** A. A. LG Hamburg wistra 2011, 155, 159; AG Bayreuth MMR 2010, 266, 267.

**56** S. hierzu bereits oben bei und mit Fn. 48.

**57** BVerfGE 120, 274, 321 weist ausdrücklich darauf hin, dass die im dortigen Verfahren angegriffene polizeirechtliche Norm »nicht unmittelbar der Gewinnung *revisionsfester* Beweise für ein Strafverfahren« diente (Hervorhebung hier). Vgl. ferner Brodowski/Freiling (Fn. 5), S. 126.

**58** Schirrmacher FAS Nr. 40 vom 9. 10. 2011, S. 12; Rieger FAS Nr. 40 vom 9. 10. 2011, S. 41.

**59** LG Hamburg MMR 2008, 423, 425 m. abl. Anm. Bär; Becker/Meinicke StV 2011, 50, 52; Braun jurisPR-ITR 3/2011 Anm. 3; Th. Böckenförde JZ 2008, 925, 934 bei und mit Fn. 96; Kudlich GA 2011, 193, 196.

**60** S. hierzu oben II.4. bei und mit Fn. 24.

**61** BVerfGE 120, 274, 310 verneint dennoch einen Eingriff in Art. 13 GG. Hiergegen ist bereits eingewandt worden, dass auch sonst die zufällige Lage eines Beweismittels – innerhalb oder außerhalb einer Wohnung? – entscheidendes Kriterium für die Betroffenheit von Art. 13 GG ist (Vogel/Brodowski StV 2009, 632, 633). Nach BVerfGE 109, 279, 309 erfasst Art. 13 GG auch ausdrücklich Eingriffe in die räumliche Sphäre auf nicht-physische Weise – z. B. durch technische Hilfsmittel. Daher ist es schlicht systemwidrig, dass eine Quellen-TKÜ auch dann nicht an Art. 13 GG zu messen oder wenigstens eine Schutzbereichsverstärkung des Art. 10 GG vorzunehmen sei, wenn sich das betroffene informationstechnische System in einer Wohnung befindet.

**62** Zu den insoweit fehlenden Begleiteingriffen s. oben II.3. bei und mit Fn. 21.

**63** Übereinkommen vom 29. 5. 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union, AblEG C 197 vom 12. 7. 2000, S. 3.

**64** Vgl. Vogel/Burchard in: Grützner/Pötz/Kreß (Hrsg.) Internationale Rechtshilfe in Strafsachen (Stand: Juli 2011) § 77 IRG Rdn. 38.

**65** Vgl. Grützner/Pötz/Kreß/Vogel/Burchard (Fn. 64) § 77 IRG

## V. Die Unzulässigkeit einer strafprozessualen Online-Überwachung

Bei allem Streit über die Zulässigkeit einer auf §§ 100 a, 100 b StPO gestützten Quellen-TKÜ ist es inzwischen einhellige Auffassung, dass es keine strafprozessuale Eingriffsgrundlage gibt für eine Online-Durchsicht und Online-Überwachung, d. h. für eine Infiltration eines informationstechnischen Systems und das Abgreifen solcher Daten, die in keinem Zusammenhang mit einer laufenden Telekommunikation stehen.[66] Daher kann das Anfertigen der Screenshots, wie in diesem Fall durch die Ermittlungsbehörden geschehen, auch nicht hypothetisch auf eine andere Eingriffsgrundlage gestützt werden.

Es bleibt die Frage nach einem Verwertungsverbot dieser rechtswidrig gewonnen Beweismittel: Eine explizite gesetzliche Regelung fehlt, so dass nach der – nicht unbestrittenen – Rechtsprechung zwischen dem Strafverfolgungsinteresse einerseits und der Schwere des Verstoßes sowie der persönlichen Betroffenheit des Beschuldigten (Rechtskreistheorie) andererseits abzuwägen ist (Abwägungslehre). Angesichts des evidenten, sich aufdrängenden Exzesses der Ermittlungsbehörden, die sich zudem über die expliziten Vorgaben des amtsrichterlichen Beschlusses hinwegsetzten, schlägt hier die Waage in die Richtung eines Beweisverwertungsverbots aus.[67] Angesichts der fehlenden technischen Absicherung der hier und auch in anderen Ermittlungsverfahren eingesetzten Spionagesoftware spricht sogar viel für ein Beweisverwertungsverbot bezüglich später beschlagnahmter Rechner und Datenträger der Betroffenen:[68] Diese Software bot den Ermittlungsbehörden nämlich die technische Funktionalität, beliebiges – also auch belastendes – Material ohne Weiteres auf dem Rechner des Beschuldigten zu hinterlegen, ohne dass hiergegen durch technische oder organisatorische Verfahrenssicherungen Vorsorge getroffen worden wäre.

Trotz dieses Exzesses drohen den Ermittlungsbeamten jedoch keine strafrechtlichen Folgen. Die Auffassung *Florian Albrechts*, diese hätten sich gem. § 202 a StGB strafbar gemacht,[69] überzeugt nicht: Die Infiltration des Rechners des Beschuldigten war durch einen amtsrichterlichen Beschluss zur Durchführung einer Quellen-TKÜ gestattet. Weil mit dieser – nach Auffassung der Rechtsprechung zudem rechtmäßigen – Infiltration zwangsläufig auch die Administratorenrechte übernommen werden müssen, sind sämtliche Zugangssicherungen durch diesen Schritt bereits überwunden. Exzessive, rechtswidrige Datenzugriffe erfolgen dann gerade nicht »unter Überwindung der Zugangssicherung« und unterfallen somit nicht dem Tatbestand des § 202 a StGB.

## VI. Fazit

Eine dezidierte Analyse des *obiter dictum* des Urteils des BVerfG über die präventive Online-Durchsuchung zeigt, dass §§ 100 a, 100 b StPO gerade keine taugliche Eingriffsgrundlage darstellt für eine Quellen-TKÜ, bei der eine Spionagesoftware auf den Rechner des Beschuldigten aufgespielt wird. Der hierbei erfolgende Begleiteingriff jedenfalls in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme erfordert eine restriktive gesetzliche Regelung, die der Gesetzgeber bis heute nicht geschaffen hat.[70] Dessen Untätigkeit rechtfertigt es auch nicht,[71] *contra legem parlamentariam* die Quellen-TKÜ richterrechtlich zu legitimieren, selbst wenn man mit guten Gründen diese Maßnahme rechtspolitisch für notwendig und sinnvoll erachtet.

Wiss. Ang. *Dominik Brodowski* LL.M. (UPenn), Tübingen

Rdn. 28. Zeitungsberichten zufolge führte Deutschland jedoch auf Ersuchen der Schweiz eine Quellen-TKÜ gegen eine in der Schweiz residierende Schweizerin durch, vgl. Schmid/Baumgartner NZZ Online, http://bit.ly/okVwaV (Stand: 16. 10. 2011).

**66** S. nur Braun jurisPR-ITR 3/2011 Anm. 3; F. Albrecht JurPC Web-Dok. 59/2011 Abs. 30 sowie Meyer-Goßner/Schmitt (Fn. 7) § 100 a Rdn. 7 b; SK-StPO/Wolter (Fn. 30) § 100 a Rdn. 30, jew. m. w. N.

**67** So auch F. Albrecht, JurPC Web-Dok. 59/2011 Abs. 21.

**68** Vgl. Rieger FAS Nr. 40 vom 9. 10. 2011, S. 41, 41 f.

**69** F. Albrecht, JurPC Web-Dok. 59/2011 Abs. 23.

**70** Ein Gesetzesvorschlag ist zu finden in Brodowski/Freiling (Fn. 5), S. 144 f.

**71** So aber – für eine Übergangszeit – KK-StPO/Nack (Fn. 30) § 100 a Rdn. 27; hiergegen zu Recht F. Albrecht JurPC Web-Dok. 59/2011 Abs. 30; SK-StPO/Wolter (Fn. 30) § 100 a Rdn. 30.